

Cybersection

Federal Regulators Release Revised Management IT Booklet

In November, the Federal Financial Institutions Examinations Council (FFIEC) issued its **revised Management booklet**, which is part of the IT Examination Handbook. The Management booklet provides guidance to examiners regarding how IT governance and risk management relates to the overall governance and risk management strategy of financial institutions.

Data Breach Protocol

Pennsylvania, like most other states, requires any for-profit or non-profit business organization and any state or local government agency or political subdivision that maintains, stores or manages computerized data containing personal information to notify commonwealth residents affected by a data breach without unreasonable delay (Breach of Personal Information Notification Act, 73 P.S. § 2301 et seq).

Numerous sources are available to help businesses and organizations develop response plans that can help manage the impact of a data breach. However, there are some basic concepts that a business can include in its response plan:

- **Response Team** – Establish a response team to handle data breach incidents. Include IT personnel, company or agency leaders, attorneys, human resources personnel, public relations staff, and any applicable third-party vendors.
- **Incident Assessment** – Determine when and where the data breach took place as well as what data have been compromised. Establish how many individuals could be or have been affected by the breach.



- **Analysis** – Analyze the affected system to determine if there are further weaknesses that may be exploited, and fix any issues that may have caused the breach.
- **Communications Plan** – Decide the best method for notifying and communicating with affected individuals as well as the message that should be delivered to the public.
- **Law Enforcement** – Notify local, state and/or federal law enforcement, if the nature of the breach requires it.

Cybersecurity Act of 2015

Congress recently enacted the Cybersecurity Information Sharing Act of 2015, which provides for the voluntary sharing of cybersecurity threat information between private and public entities and the federal government, including liability protections. This new law includes the creation of a process that will allow information systems to share cybersecurity threat details automatically, requires an assessment of the federal government's cybersecurity workforce, and addresses improvement of cybersecurity in the health care industry. You can download a copy of the law [here](#).

DoBS Staff Recognized at PA Digital Government Summit



The department's Chief Information Security Officer, Paul Metzler (center), received a "Pennsylvania Excellence in Technology Award" at the PA Digital Government Summit in Harrisburg in December. He was recognized for his role in the department and his work with the newly formed DoBS Cybersecurity Task Force.



He was joined at the award ceremony by Secretary Robin L. Wiessmann (third from right) and other DoBS colleagues.



Reminder: Depositories, Estates, and Revenue

It has come to the attention of the Department of Banking and Securities that some financial institutions may not be fully aware of the PA Department of Revenue requirements regarding joint account information or trust deposits following the death of a customer. In addition, the Department of Revenue would like to share some suggestions regarding the granting of access to safe deposit boxes.

Joint Account/Trust Deposit

This is a reminder that financial institutions are required by law to notify the Department of Revenue, within 10 days after knowledge of a death, of the existence of a joint account or trust deposit held by the deceased. This notice is required both of Pennsylvania institutions and out-of-state institutions with branches located in Pennsylvania. The notice requires the name of the decedent, the date of the creation of the account, the titling of the account as of the date of death, the date of death balance and the name and address of the survivor or survivors to the account. No notice is required if the date of death balance is less than \$300.

Safe Deposit Boxes

Entry into a deceased customer's safe deposit box requires that the representative of the estate mail a notice providing pertinent information to the Department of Revenue at least seven (7) days prior to the expected entry into the box. The Department of Revenue requests that financial institutions accept its written or verbal communication to confirm receipt of entry notification regarding entry to the safe deposit box. It is noted that representatives of the estate can also go to the U.S. Postal Service website and enter the tracking number to verify the Department of Revenue has received the notice regarding entry notification. A print-out of the delivery confirmation from the Postal Service website could also be accepted as receipt of entry notification.

